

Summary of Information Request

Credit Union

DFI takes steps to protect the confidentiality of personal information, to the extent permitted by law. However, all information collected by DFI becomes a public record and may be subject to inspection and copying by the public, unless an exemption or other protection in law exists. A copy of our privacy policy is available upon request.

DIRECTIONS: Reports and information should be prepared as of the exam cutoff date. Management may wish to discuss individual credit union report options with the Examination Supervisor or the EIC prior to the exam start. If you cannot provide the documents or answers requested, please indicate why. If a particular question is not applicable, simply indicate N/A.

AUDIT:

- 1.1. Indicate the name of the contact person(s) to obtain the minutes of the board of directors, audit committee, and examining committee?
- 1.2. A copy of the internal auditor's resume or brief biographical worksheet stating training and experience.
- 1.3. A copy of all internal and external audit reports and reviews completed since the last Information Systems Examination.
- 1.4. A copy of audit schedules for the past two years and the future.
- 1.5. A copy of the audit standards used, and/or audit tasks outlines (work programs).
- 1.6. A copy of the internal auditor's job description and/or a listing of all duties (audit and other) performed by the internal auditor.
- 1.7. List the audit software used. Indicate: program name, applications the software audits, software vendor or developer, frequency of use, and date last used.

MANAGEMENT:

- 2.1. List management committees that consider Information Systems related matters and provide a brief description of their responsibilities. Who should the examiner contact to review the minutes of these committees?
- 2.2. Describe any significant plans for changes in Information Systems management personnel, software, hardware or operating procedures within the next 12 months.

- 2.3. A copy of the organization chart for the data center. Also, an organization chart which includes the audit department and security personnel.
- 2.4. Describe your procedures and controls for using report generators and the reports created using them.
- 2.5. Provide a copy of contracts with outside servicers.
- 2.6. Were contracts with servicers reviewed by your legal counsel?
- 2.7. Provide a copy of the institution's IS and/or Computer Security Policy(s).
- 2.8. Provide documentation of senior management's periodic analysis of the financial condition of its significant vendor(s) and/or servicers.
- 2.9. List membership in software users' groups.
- 2.10. Provide details of hardware and/or software amortization.
- 2.11. If financial models are used, briefly describe the method(s) to ensure the validity of assumptions, data, and calculations used in the model(s).
- 2.12. Provide a copy of the institution's last insurance review (Please put an "X" next to bonds and insurance which you have on the following list) and coverage amounts:

Description	Coverage Amount
Blanket bond	
Excess Employee Dishonesty bond	
Equipment and Facilities insurance	
Media Reconstruction insurance	
Electronic Funds Transfer insurance	
Business Interruptions insurance	
Errors and Omissions insurance	
Extra Expense and/or Backup Site Expense insurance	
Items in Transit insurance	
Other Probable Risk insurance	
Other, please list	

SYSTEMS AND PROGRAMMING:

- 3.1. Please complete the attached "APPLICATION CHECKLIST"(Page 4).
- 3.2. Describe your procedures for implementing software vendor provided program updates, releases, changes, and emergency program changes.
- 3.3. Describe or provide a copy of your policy covering procedures and approvals required for setting and/or changing parameters (interest rates, service charges, etc. on loans and deposits).
- 3.4. Provide a copy of the contract(s) or license agreement(s) for application software.
- 3.5. Describe procedures and controls for vendors' dial-in access to your system(s) to make software changes. Do modems have dial-back capabilities and are they in use?
- 3.6. Indicate update and/or release number of the applications software being used. Have all software updates and releases been installed? If not, why not?

APPLICATIONS CHECKLIST

PLEASE INDICATE WHERE YOU OBTAINED THE PROGRAMS FOR EACH APPLICATION. IF THE PROGRAMMING WAS DONE IN HOUSE PLEASE INDICATE. IF YOU DO NOT OFFER THE APPLICATION PUT "NOT OFFERED" NEXT TO THE APPLICATION.

Applications	Software Vendor/Package Servicer - Processing Site	In-house/ Turnkey	Serviced
General Ledger			
Investments			
Loans:			
Commercial			
Construction			
Mortgage			
Home Equity			
Installment			
Student			
Check Credit			
Shares:			
Draft			
Savings			
Time			
Other:			
CIF			
Payroll			
Other: (List)			

COMPUTER OPERATIONS:

- 4.1. Provide a list of all compilers and program/data altering utility programs on your system.
- 4.2. Please complete the attached "SYSTEM DESCRIPTION SCHEDULE" (Page 6). If the equipment listed is leased please provide a copy of the lease.
- 4.3. Provide a list of the backup tapes, disks, documentation, supplies, etc. kept at your off-premises storage facility.
- 4.4. If you provide services for non-financial institution or financial institution customers, please complete the requested information on the attached "STATISTICAL DATA SCHEDULE" (Page 7).
- 4.5. Provide a copy of the contract(s) for services provided for non-financial and financial institution customers listed.
- 4.6. Provide a copy of the service agreement(s) for all major hardware.
- 4.7. Provide a copy of your Emergency Plan (may be part of your contingency plan).
- 4.8. Provide a copy of your Contingency plan.
- 4.9. Provide a copy of the written agreement with your backup processing site.
- 4.10. Provide a copy of the results of the last test of your contingency plan/backup site.
- 4.11. For applications serviced by others, do you subscribe to the disaster recovery services offered by that servicer? If so, please provide a copy of the contract. If not, what other arrangements have been made?

SYSTEM DESCRIPTION SCHEDULE

	COMPUTER	COMPUTER	COMPUTER	COMPUTER	COMPUTER
MANUFACTURER					
MODEL					
LEASED FROM					
MEMORY					
OP-SYSTEM &					
VERSION #					

- HOW MUCH DISK STORAGE DO YOU HAVE? _____ PERCENTAGE UTILIZED? _____%
- APPROXIMATELY HOW MANY TERMINALS AND/OR PCs EMULATING TERMINALS ARE ON YOUR SYSTEM?
- ARE THEY CONNECTED TO THE SYSTEM VIA LEASED LINES _____ DEDICATED LINES _____ AND/OR DIAL UP LINES _____? (INDICATE BY PLACING AN "X").
- APPROXIMATELY HOW MANY ATMs ARE DIRECTLY CONNECTED TO YOUR SYSTEM?
- ARE YOU A MEMBER OF AN ATM NETWORK(S)? _____ IF SO PLEASE NAME:
- IF YOU USE PCs PLEASE INDICATE APPROXIMATELY HOW MANY AND WHAT THEY ARE USED FOR:
- DO YOU HAVE A "LAN(S)" AND/OR "WAN"(S)? _____. IF YOU DO DESCRIBE USE.
- INDICATE THE OFF-PREMISES LOCATION WHERE BACKUP DATA FOR EACH OF YOUR COMPUTER SYSTEMS IS STORED.

STATISTICAL DATA SCHEDULE

Code	Application	Application Not Offered	Batch Process	Inquiry On Line	Update Real Time
A.	Commercial Loans				
B.	Installment Loans				
C.	Mortgage Loans				
D.	Share Deposits				
E.	Time and/or Savings Deposits				
F.	General Ledger				
G.	CIF (Customer Info. File)				
H.	Elec. Funds Trans. (ACH & ATM)				
Z.	Other: Payroll				
Z1	POS and/or Credit Cards,				
Z2	Accts. Receivable,				
Z3	Securities,				
Z4-7	Please Describe:				

X = All Processing I = Inquiry Only M = Memo Posting F = File Maintenance

Example: Demand deposits may be batch processed and have master file changes entered on line and teller items entered as memo posts. CIF may be inquiry only and ATM services may be on line real time.

D.	Share Deposits		X	M	F
G.	CIF			I	
H.	ATM services				X

FINANCIAL INSTITUTIONS YOU SERVICE - PUT AN "X" FOR EACH SERVICE THEY RECEIVE

APPLICATION (By Code) FROM THE ABOVE LISTING

Name City and State	A	B	C	D	E	F	G	H		Z	Z1	Z2	Z3	Z4	Z5	Z6	Z7

FOR ALL CUSTOMERS THAT ARE NOT FINANCIAL INSTITUTIONS PLEASE INDICATE THE SERVICE(S) THEY RECEIVE AND THE NUMBER OF CUSTOMERS RECEIVING THE SERVICE:

SERVICE RECEIVED

NUMBER OF CUSTOMERS

TELEPROCESSING /DATA SECURITY:

- 5.1 If not detailed in your security policy(s), provide a description or a copy of the policy describing controls for dial-in access to your computer systems. Such as:
- a. Senior management approval of dial-in access;
 - b. Limits placed on what activities can be performed;
 - c. Automatic callback to identify dial-in terminal/user;
 - d. Other controls.
- 5.2 Provide a list of all users of each computer system. The list(s) should detail the users' name or user ID and access authority.
- 5.3 Describe password parameter controls, for example:
- a. Number of characters required.
 - b. Must passwords have both alpha and numeric characters?
 - c. Are repeating characters allowed?
 - d. Can a password be used more than once by a user?
 - e. Can a password that is similar to one that has been used be used?
 - f. Are certain names and words not allowed as passwords?
 - g. How often are passwords changed?
 - h. Are passwords suppressed from all output?
 - i. Other?
- 5.4 Is system access restricted by:
- a. Physical terminal locks?
 - b. Passwords?
 - c. Unique operator identification?
 - d. Functions available to only specific terminals?
 - e. Automatic log-off if left unattended? For how long?
 - f. Automatic log-off after _____ (number) failed access attempts?
 - g. Time of day and day of week?
 - h. Removal from the system of users who have not signed in for _____ (number) days?
- 5.5 How frequently are individuals' system access levels reviewed for appropriateness?
- 5.6 Provide documentation that reflects review of reports detailing security violations such as failed access attempts.

ELECTRONIC FUNDS TRANSFER (ATM/POS/ACH):

- 6.1 Provide copies of contracts for ATM network services to which the institution subscribes. Also provide copies of contracts with ATM card vendors/manufacturers you use.
- 6.2 Provide a blank copy of ATM/POS agreement(s) with your depositors. Also provide a blank copy of the ATM/POS agreement(s) with merchants.
- 6.3 Describe below or provide a copy of the institution's policy covering ATM card and PIN issuance procedures.

MICROCOMPUTERS:

- 7.1 Provide a copy of the credit union's microcomputer policy.

NETWORKS (LANS/WANS):

- 8.1 Provide a schematic of your network topography – identify computer locations and interfaces
- 8.2 Provide a copy of the written policy(s), standards and procedures for network design, support and security.
- 8.3 Provide a description of the network administrator's and network security officer's duties and responsibilities within your institution.
- 8.4 Provide a listing of all network users, and their access capabilities and rights.
- 8.5 Provide a description of network password administration procedures.
- 8.6 Provide a copy of documentation of the last review of network software vendor(s) financial stability, if not provided in item 2.8.
- 8.7 Provide a copy of your contract(s) with the network software vendor(s) who provide network programming and hardware support.
- 8.9 Describe below network password parameter controls:
a. How often must passwords be changed?
b. Are passwords suppressed from all output?
- 8.10 Is network(s) access restricted by:
a. Physical terminal locks?
b. Passwords?
c. Password encryption?
d. Unique operator identification?
e. Limited access to security tables (access codes, passwords)?
f. Functions available to specific terminals?
g. Automatic log-off of left unattended? For how long?
h. Automatic log-off after _____ (number) failed access attempts?
i. Time of day and day of week?
j. Removal from the system of users who have not signed on for _____ (number) days?
- 8.11 If not detailed in your security policy, provide a description or copy of the policy describing controls for dial-in access to your network. Such as:
a. Senior management approves all dial-in access;
b. Limits placed on activities that can be performed;
c. Automatic call-back to identify dial-in terminal/user;
d. Other controls.
- 8.12 Describe anti-virus procedures or provide a copy of your policy which addresses this issue.
- 8.13 Describe method(s) of identifying and backing-up critical/sensitive network data files and application programs. Provide a list of the backed up network data files and applications programs.

- 8.14 How frequently are individual system access levels reviewed for appropriateness?
- 8.15 Describe method for replacing/backing-up critical network hardware.

CUSTOMER SERVICE (CLIENTS SERVED):

- 9.1 Copy of each TYPE of contract used for processing financial institution'(s) data.

ELECTRONIC BANKING:

- 10.1 Please provide the electronic banking contact' name, title, and phone number. In addition, please provide the organizational chart of electronic banking personnel and their job description.
- 10.2 Please list all electronic banking platforms utilized and system topology maps including servers, routers, firewalls, and other supporting system components.
- 10.3 Copy of any risk analysis or reviews of electronic banking activity.
- 10.4 Provide list of pending lawsuits/contingent liabilities with potential losses relating to electronic banking activities.
- 10.5 Provide due diligence reviews of third party providers, contractors, support vendors, or any other parties.
- 10.6 Provide any system security reviews conducted by third parties.
- 10.7 Copy of all contracts/agreements with vendors, customers, third-parties, etc.
- 10.8 Copy of insurance policies covering electronic banking activities such as blanket bond, liability coverage, errors and omissions, and any riders relating to electronic banking activities.
- 10.9 Copy of strategic plan and feasibility studies (cost/benefit analysis), test plans and results, deployment plans and reviews relating to electronic banking activity.
- 10.10 Provide any reports that measure or analyze actual performance to projections including performance in strategic areas such as deposit growth and technical areas, or the ability to process the current level of transactional or support activity.
- 10.11 Copy of general policies relating to electronic banking activity (defining bank's trade area, accepting account applications, compliance with Financial Record-keeping and BSA requirements, etc.)
- 10.12 Copy of specific policies and procedures relating to electronic banking operations for items such as new products, services, or delivery channel- i.e. directly related to specific platforms (for example: internet banking, phone banking, etc.) and applications such as e-mail, bill payment, dollar limits per transaction, settlement guidelines, overdrafts, uncollected funds, reconciliation procedures, disclosures, among others.
- 10.13 Copy of policies for reporting and responding to electronic banking platform system delays, problems, and logbook.
- 10.14 Copy of policies or written procedures relating to electronic banking security program.
- 10.15 Copy of the most recent system reports provided by electronic banking platforms used to track nature, volume, trends, and unauthorized attempts into the credit union system.
- 10.16 Copy of audits relating to electronic banking. Provide external auditor's engagement letter and management letter including scope and findings. For internal audit, please provide audit schedule, scope, and auditors resume.
- 10.17 List of report of authorized users and levels of access for electronic banking platforms, including officers, employees, system vendors, customers, and other users.

- 10.18 Copy of exception reports, review of logs, and the name of the employee who reviews subject reports and when.
- 10.19 Copy of the credit union's back-up/contingency planning for electronic banking platforms.
- 10.20 Copy of electronic banking training (for example: products, services, informational) schedule with dates, attendees, and topics. Provide copies of any educational material and customer agreements.

MISCELLANEOUS:

- 11. Copies of the following:
 - Wire Transfer Policy
 - Privacy Policy
 - Computer User List for critical bank applications and security code book
 - Most recent quarter-end financial statement
 - List of board of directors, identify those which are outside directors